UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,240	06/26/2001	Zheng Qi	BRCMP013A	3459

7590 06/29/2005

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,240	QI ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-20,22-28 and 40* is/are pending in the application.

4a) ~~Of the above~~ claim(s) *7,21 and 29-39* is/are ~~withdrawn from consideration~~. cancelled

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-20,22-28 and 40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1, 15, and 29 were amended. Claims 7, 21, and 29-39 were cancelled. Claim 40 was added. Claims 1-6, 8-20, 22-28, and 40 are pending.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Information Disclosure Statement

The IDS applicant submitted on 5/2/2005 have been considered.

Response to Amendment

In light of applicant's amendments to the specification and claims, the examiner withdraws the previous office action's objection to the specification and 112, second paragraph rejections of the claims. The examiner also notes that the amendments to the claims raise new issues. As a result, new rejections will be made as appropriately below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 8-20, 22-28, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (US 6,769,063) in view of Windirsch (US 6,760,439) and further in view of Callum (US 6,320,964).

Claims 1 and 15:

Kanda discloses a cryptographic engine as per claim 1 for performing cryptographic operations on a data block (col 1, lines 8-15). Kanda also discloses an integrated circuit layout associated with a cryptography engine as per claim 15 for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (col 1, lines 8-15). Kanda further discloses the cryptographic engine and the integrated circuit layout comprising:

1. A key scheduler configured to provide keys for cryptographic operations (col 7, lines 11-25).
2. Expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (col 15, lines 8-20 and Figure 8A-8D).
3. Permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (col 1, lines 31-46).

Kanda does not explicitly disclose:

1. A two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level, wherein the two-level multiplexer circuitry avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle.
2. Permutation logic coupled to the expansion logic.

However, Windirsch discloses a two-level multiplexer circuitry including a multiplexer on a first level coupled to a multiplexer on a second level (col 1, lines 35-47), wherein the two-level multiplexer circuitry avoids swapping of data loaded from a previous round of cryptographic processing without incurring an extra clock cycle (col 2, lines 36-50). Further, Callum discloses permutation logic coupled to the expansion logic (Figure 3, items 319 and 320).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have incorporated Windirsch and Callum's teachings with Kanda's according to the limitations recited in claim 1. One of ordinary skill would have been motivate to incorporate Windirsch's teachings because he discloses that it would allow for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, 1st paragraph) and allow for simultaneous processing of a number of data streams (col 2, lines 12-16). One of ordinary skill would have been motivated to incorporate Callum's teachings because he discloses that his teachings would allow a cryptography engine to better handle instruction-intensive bit permutation and thereby achieve greater cryptography speed (abstract).

Claims 2 and 16:

Kanda further discloses the cryptographic engine, further comprising an Sbox configuration to alter a third bit sequence corresponding to the portion of the data block

by compacting a size of the third bit sequence and altering the third bit sequence using Sbox logic (col 3, lines 31-52; col 10, last paragraph; and col 11, 1st paragraph).

Claims 3 and 17:

Kanda further discloses the cryptography engine, wherein the cryptography engine is a DES engine (col 14, lines 15-28).

Claims 4 and 18:

Windirsch further discloses two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level (Fig 1, items 13, 25, 29, and 33). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15

Claims 5 and 19:

Kanda further discloses the cryptography engine, wherein the first bit sequence is less than 32 bits (col 2, lines 1-21).

Claims 6 and 20:

Kanda further discloses the cryptography engine, wherein the first bit sequence is four bits (col 17, lines 9-28).

Claims 8 and 22:

Callum further teaches the cryptography engine, wherein the expansion logic and the permutation logic are associated with DES operations (col 3, lines 32-47 and Fig 3, items 319 and 320). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15.

Claims 9 and 23:

Windirsch further teaches pipelining being used in an encryption/decryption device (col 2, lines 12-35). One of ordinary skill would be motivated to incorporate Windirsch's teachings of pipelining into the combination system of Kanda, Windirsch, and Callum for the same reasons as for claims 1 and 15.

Claims 10 and 24:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a plurality of stages (col 1, lines 18-67).

Claims 11 and 25:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a determination stage (col 15, lines 21-33).

Claims 12 and 26:

Callum further discloses the cryptography engine, wherein the key scheduler comprises a shift stage (col 4, lines 46-67 and col 5, lines 1-5). The motivations for combining the teachings of Kanda, Windirsch, and Callum are the same as for claims 1 and 15.

Claims 13 and 27:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a propagation stage (col 2, lines 1-21).

Claims 14 and 28:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a consumption stage (col 3, lines 30-51).

Claim 40:

As per claim 40, Kanda, Windirsch, and Callum do not explicitly disclose wherein the multiplexer on the first level loads the data block in response to a first signal value, and further loads data from a previous round of cryptographic processing in response to a second signal value, and the multiplexer on the second level swaps the loaded data from the previous round of cryptographic processing in response to a third signal value, and further fails to swap the loaded data from the previous round of cryptographic processing in responds to a fourth signal value. However, the examiner submits that the above limitation is obvious to the combination invention of Kanda, Windirsch, and Callum. Notice that Windirsch discloses that his teachings allow for swapping of context without incurring additional delay (col 2, lies 37-50). Further, Windirsch discloses the multiplexers being used to select the data signals (col 5, lines 4-21). These teachings by Windirsch read on the limitations as recited in claim 40.

Claims 4 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (US 6,769,063) in view of Windirsch (US 6,760,439) and further in view of Callum (US 6,320,964) and Steinman et al (US 6,591,349).

Claims 4 and 18:

Kanda does not explicitly teach two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on a second level. However, Steinman teaches 2-to-1 multiplexer usage (col 3, last paragraph and col 4, 1st paragraph). It would have been obvious to one of ordinary skill at the time the applicant's invention was made to employ

Steinman's teachings within the combination system of Kanda, Windirsch, and Callum as it would allow increased performance of a computer memory system by reducing lost clock cycles (Steinman's abstract). It would have been obvious to one of ordinary skill to have two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level because it would allow for increased performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. The speed up in clock cycle improves the performance of DES.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100